BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-139735
(43)Date of publication of application : 27.05.1997

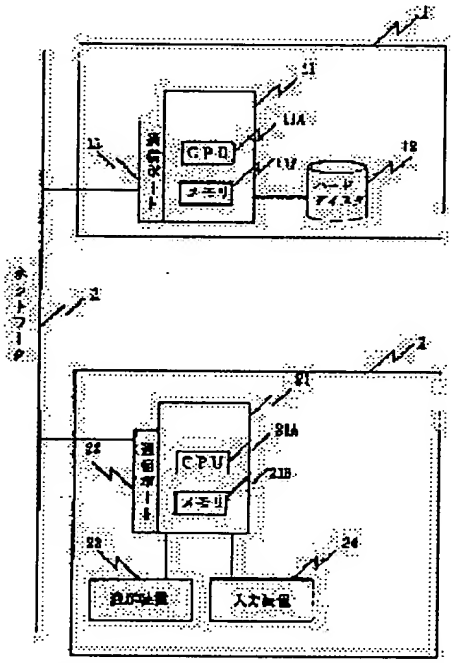
(51)Int.Cl. H04L 9/08
G06F 15/00
G09C 1/00
G09C 1/00

(21)Application number : 07-297026
(22)Date of filing : 15.11.1995

(71)Applicant : HITACHI SOFTWARE ENG CO LTD
(72)Inventor : FUJIOKA HIDEKI

(54) CIPHERING DATA COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To secure security of data communication by incorporating a relay service program to realize chiphering data communication to memories of a server and a client, respectively.
SOLUTION: A server 1 and a client 2 are connected via a network 3. A relay service program to realize ciphering data communication is incorporated in memories 11B, 21B of the server 1 and the client 2. Thus, an application program of its own computer ciphers data to be sent to an application program of other computer. Then data received from the application program of the other computer are decoded and given to the application program of its own computer.



LEGAL STATUS

[Date of request for examination] 18.06.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－139735

(43)公開日　平成９年(1997)５月27日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｂ
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ｂ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｂ
		６６０	7259－5Ｊ			６６０Ｅ

審査請求　未請求　請求項の数３　ＯＬ　（全 12 頁）

(21)出願番号　特願平7－297026

(22)出願日　平成７年(1995)11月15日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地

(72)発明者　藤岡　秀樹
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(74)代理人　弁理士　秋田　収喜

(54)【発明の名称】　暗号化データ通信システム

(57)【要約】

【課題】　既存のアプリケーションやオペレーティングシステムに変更を加えることなく、ネットワーク上を流れるデータを暗号化し、データ通信のセキュリティを確保する。

【解決手段】　２つのコンピュータ上で、それぞれ中継サービスプログラムを稼動させておき、この中継サービスでデータを暗号化させ、ネットワーク経由で送受信する。

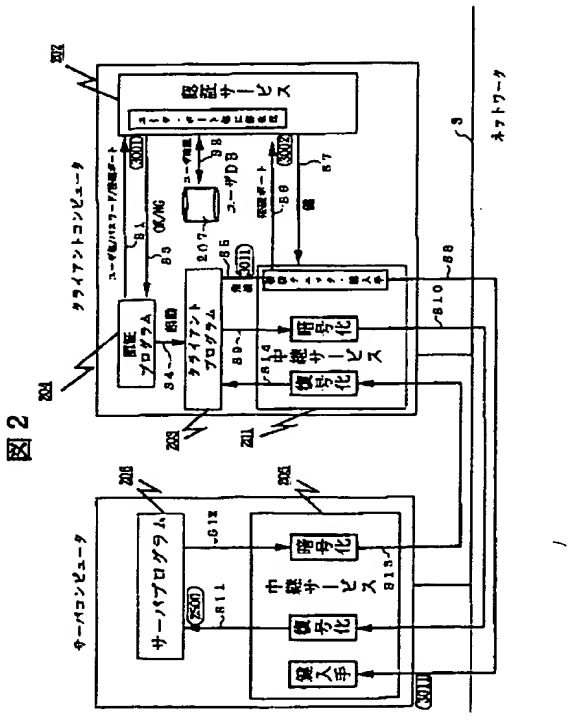


図２

【特許請求の範囲】
【請求項１】　ネットワーク経由でデータを通信する少なくとも２つのコンピュータを備えた暗号化データ通信システムであって、
前記各コンピュータは、自コンピュータのアプリケーションプログラムが他方のコンピュータのアプリケーションプログラムに送信するデータを暗号化し、他方のコンピュータのアプリケーションプログラムから受信したデータを復号し、自コンピュータ内のアプリケーションプログラムに渡す中継サービス処理手段を備えることを特徴とする暗号化データ通信システム。
【請求項２】　前記各コンピュータは、自コンピュータのアプリケーションプログラムがデータを送信する際に、該アプリケーションプログラムを使用するユーザの認証処理によってユーザ毎の暗号鍵を生成し、中継サービス処理手段に転送する認証処理手段をさらに備えることを特徴とする請求項１記載の暗号化データ通信システム。
【請求項３】　前記中継処理サービス処理手段は、所定の記録媒体に記録されたプログラムとして各コンピュータ内に組み込まれるものである請求項１または２記載の暗号化データ通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークに接続された複数のコンピュータ間でデータの送受信を行う際に、既設のオペレーティングシステムや通信用プログラムに変更を加えることなく、クライアントコンピュータとサーバコンピュータ間で通信されるデータのセキュリティを確保するための暗号化データ通信システムに関するものである。
【０００２】
【従来の技術】コンピュータの性能の向上、ネットワークへの接続が進むにつれ、情報を複数のコンピュータに分散させて保存し、ネットワークに接続している別のコンピュータから参照するという分散コンピューティングが行われてきている。
【０００３】このように、ネットワークに接続されたコンピュータ間で情報をやり取りする場合、サーバ・クライアント型の形態で情報通信を行うが、この時ネットワーク上には情報がそのまま流れるため、人事情報や企業間での情報のやり取りを行った場合、傍受される危険性が高い。
【０００４】そこで、従来は、これを防ぐために、
（１）一旦暗号化した情報を電子メールやファイル転送で配送する、（２）セキュリティルータに代表される暗号化機能を持ったハードウェアを利用し、ルータ間で暗号化した情報を転送する、（３）「Ｋｅｒｂｅｒｏｓ」のように、オペレーティングシステム自身にセキュリティ機能を持たせ、通信時のセキュリティを確保する、などの方策が実施されている。
【０００５】また、特開平３－８０７５２号公報に開示されているように、端末が交換機に直接接続されている場合に、別の交換機に接続された端末間での通信を傍受されないように、交換機内に暗号化機能を付加したものがある。
【０００６】
【発明が解決しようとする課題】しかしながら、前記（１）の方法でデータを通信するシステムにあっては、データ自身の暗号化は通信用プログラムと全く別の部分で行うか、またはサーバコンピュータやクライアントコンピュータ上で動作する通信用プログラム内に暗号化機能を組み込む必要がある。しかし、通信用プログラムと全く別の部分（暗号化プログラム）で暗号化するようにした場合、既設の通信用プログラムの中に暗号化プログラムを呼び出す処理を追加しなければならなくなり、一般ユーザにおいては実現不可能である。また、通信用プログラム内に暗号化機能を組み込むようにした場合、アプリケーション開発者にとって負担が大きいという問題がある。
【０００７】次に、（２）の方法でデータを通信するシステムにあっては、ルータ間のセキュリティは確保されているが、ルータ内のネットワーク上には「生のデータ」が流れるため、通信のセキュリティを確保することはできない。
【０００８】この場合、サーバコンピュータやクライアントコンピュータ内に、暗号化機能を実現するハードウェアを追加することが考えられるが、ハードウェアの追加空間が常に確保されているとは限らず、追加空間が無い場合は通信のセキュリティを確保することはできない。さらに、追加空間があったとしても、前記（１）の場合と同様に、既設の通信用プログラムの中に暗号化用ハードウェアを呼び出す処理を追加しなければならなくなり、一般ユーザにおいては実現不可能である。
【０００９】次に、（３）の方法でデータを通信するシステムにあっては、全ての通信にセキュリティが確保されるが、全てのコンピュータのオペレーティングシステムがセキュリティ機能を装備していることが必要になり、既存のオペレーティングシステムを利用したアプリケーションには適用できないという問題がある。
【００１０】さらに、特開平３－８０７５２号公報に開示されている方法でデータを通信するシステムにあっては、汎用計算機の端末などで扱うデータを電話回線を通じて中央の汎用計算機に一旦集めた後に転送する場合には利用可能であるが、１本の伝送媒体に複数のコンピュータが接続されているバス形式のネットワークの形態である場合、ネットワーク上に「生のデータ」が流れるため、通信のセキュリティが確保できないという問題がある。
【００１１】本発明の目的は、既設または既存のアプリ

ケーション（通信用プログラムなど）やオペレーティングシステムに全く変更を加えずに、全ての接続形態のネットワーク上で通信されるデータのセキュリティを確保することができる暗号化データ通信システムを提供することにある。

【００１２】

【課題を解決するための手段】本発明は、上記目的を達成するために、ネットワーク経由でデータを通信する各コンピュータ内に、自コンピュータのアプリケーションプログラムが他方のコンピュータのアプリケーションプログラムに送信するデータを暗号化し、他方のコンピュータのアプリケーションプログラムから受信したデータを復号し、自コンピュータ内のアプリケーションプログラムに渡す中継サービス処理手段を設けたことを特徴とする。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態を図面を用いて詳細に説明する。

【００１４】図１は、本発明を適用した暗号化データ通信システムの実施形態の一例を示すシステム構成図である。

【００１５】この実施形態は、データのセキュリティを必要とする「社員の健康管理業務」を行う健康管理システムを想定して構成されている。健康管理業務では、社員のプライバシーに関る情報を扱うため、ネットワークに流れるデータを傍受から守るために、暗号化によって通信セキュリティを確保することが必須である。

【００１６】この実施形態のシステムは、ネットワーク３で接続されたサーバコンピュータ１とクライアントコンピュータ２とで構成されている。

【００１７】サーバコンピュータ１は、ＣＰＵ１１Ａ、メモリ１１Ｂから成る端末装置１１と、社員の健康管理情報を保存しておくための外部記憶装置１２と通信ポート１３とを備えている。

【００１８】クライアントコンピュータ２は、サーバコンピュータ１と同様に、ＣＰＵ２１Ａ、メモリ２１Ｂからなる端末装置２１と、通信ポート２２、健康管理データベースの検索結果などを表示する表示装置２３、及び健康管理システムを起動するためにユーザ名称やパスワードを入力したり、あるいは健康管理データベースへの検索指示を入力する入力装置２４とを備えている。

【００１９】これらサーバコンピュータ１およびクライアントコンピュータ２のメモリ１１Ａ，１１Ｂには、暗号化データ通信を実現するための中継サービスプログラムが組み込まれている。この中継サービスプログラムは、フロッピイディスクまたはＣＤ－ＲＯＭ、またはＩＣカードなどの記録媒体によってサーバコンピュータ１およびクライアントコンピュータ２のユーザに提供されるもので、起動プログラムによって稼働状態にしたり、非稼働状態にすることができる。非稼働状態にした場合は、暗号化機能は停止される。また、中継サービスプログラムは、前記のような記憶媒体でなく、ネットワーク内の上位コンピュータあるいはサーバコンピュータからダウンロードする形式でユーザに提供される。

【００２０】図２は、中継サービスプログラムを利用してサーバコンピュータ１とクライアントコンピュータ２との間で通信を行う際のデータの流れを示したものである。

【００２１】データ転送のためのプロトコルとしては様々なものが利用可能であるが、本実施例ではＴＣＰ／ＩＰを利用する。ＴＣＰ／ＩＰでは、各コンピュータごとに、そのコンピュータ上で稼動するサービスプログラムが通信に使用するために、ポートと呼ばれる番号を持っている。

【００２２】クライアントコンピュータ１では、中継サービスプログラム２０１と、認証サービスプログラム２０２が稼動している。

【００２３】一方、サーバコンピュータ２では、中継サービスプログラム２０５と社員の健康管理情報を格納したデータベースを処理するサーバプログラム２０６が稼動している。

【００２４】ユーザは、健康管理システムを実現するためのクライアントプログラム２０３を起動する際に、必ず認証プログラム２０４を起動する。認証プログラム２０４は、クライアントコンピュータ２の表示装置上にユーザ名称とパスワードの入力を促す画面を表示する。

【００２５】ユーザが健康管理システムを使用するために、ユーザ名称とパスワードを入力すると、認証プログラム２０４は、認証サービスプログラム２０２のサービスポートである「３００１番」に対して接続し、ユーザ名、パスワードとクライアントプログラム２０３が中継サービスプログラム２０１のどのポートに接続するかを示すポート番号を転送する（Ｓ１）。

【００２６】これに対し、認証サービスプログラム２０２は、ユーザ名称とパスワードを利用してユーザＤＢ２０７に対してユーザ確認を行う（Ｓ２）。

【００２７】その結果、ユーザがユーザＤＢ２０７に予め登録されている正規の利用者であると認証された場合は、認証サービスプログラム２０２は「ＯＫ」を、認証されない場合は「ＮＧ」を認証プログラム２０４に返答する（Ｓ３）。

【００２８】認証プログラム２０４は、認証結果が「ＮＧ」の場合は再度ユーザ名とパスワードの再入力を促す画面を表示する。認証結果が「ＯＫ」の場合は、認証プログラム２０４はクライアントプログラム２０３を起動する（Ｓ４）。

【００２９】クライアントプログラム２０３は、中継サービスプログラム２０１の通信ポートである「３０１１番」に対して接続する（Ｓ５）。

【００３０】中継サービスプログラム２０１は、認証サ

ービスプログラム２０２の暗号鍵通信ポートである「３００２番」に接続し、クライアントプログラム２０３から接続されたポート番号を認証サービスプログラム２０２に渡し（Ｓ６）、そのポート番号で認証されたユーザの暗号鍵を入手する（Ｓ７）。

【００３１】その後、中継サービスプログラム２０１は、サーバコンピュータ１で稼動している中継サービスプログラム２０５の中継ポートである「３０１１番」「に接続し、認証サービスプログラム２０２から入手した暗号鍵を中継サービスプログラム２０１，２０５に固有の鍵で暗号化して中継サービスプログラム２０５にネットワーク３経由で送信する。

【００３２】サーバコンピュータ１の中継サービスプログラム２０５は、クライアントコンピュータ２の中継サービスプログラム２０１から送信されてきた「暗号化された暗号鍵」を中継サービス固有の鍵で復号し保持しておく（Ｓ８）。

【００３３】クライアントプログラム２０３は、サーバプログラム２０６に送信すべきデータを中継サービスプログラム２０１に送信する（Ｓ９）。

【００３４】送信するデータには、サーバコンピュータ側のデータベースのアクセス許可を得るためのユーザ名称とパスワードや、データベース検索のためのＳＱＬ文などがあり、これらは通常のテキスト形式で送信される。

【００３５】中継サービスプログラム２０１は、クライアントプログラム２０３から送信されてきたデータを、認証サービスプログラム２０２から入手した暗号鍵で暗号化し、サーバコンピュータ１の中継サービスプログラム２０５に転送する（Ｓ１９）。

【００３６】中継サービスプログラム２０５は、サーバプログラム２０６の受信ポートである「２５００番」に接続し、クライアントコンピュータ２の中継サービスプログラム２０１から受信したデータを、保持しておいた暗号鍵で復号し、サーバプログラム２０６に送信する（Ｓ１１）。

【００３７】サーバプログラム２０６は、受信したデータを処理した後、結果を中継サービスプログラム２０５に送信する（Ｓ１２）。

【００３８】中継サービスプログラム２０５は、受信したデータを、保持しておいた暗号鍵で暗号化し、クライアントコンピュータ２の中継サービスプログラム２０１に送信する（Ｓ１３）。

【００３９】クライアントコンピュータ２の中継サービスプログラム２０１は、受信したデータを、保持していた暗号鍵で復号し、クライアントプログラム２０３に転送する（Ｓ１４）。

【００４０】このようにうして、健康管理システムであるクライアントプログラム２０３がサーバプログラム２０６から受け取るデータは、クライアントプログラム２０３がサーバプログラム２０６と直接通信して得られるデータと全く等しいものである。

【００４１】以後、クライアントプログラム２０３とサーバプログラム２０６の間の通信は、上記の手順Ｓ９～Ｓ１４を繰り返すことにより、クライアントコンピュータ２とサーバコンピュータ２上で稼動する中継サービスプログラム２０１，２０５を経由して行われる。

【００４２】図４は、認証プログラム２０４の動作を示すフローチャートである。

【００４３】以下、図４のフローチャートを用いて、本実施例の動作を説明する。

【００４４】まず、表示装置上に、暗号化中継サービスを経由して稼働するシステム名の選択画面を表示する（ステップ３０１）。この利用システムの選択画面４０１には、図４に示すように、暗号化中継サービスを経由して稼働するシステム名が複数個表示される。ユーザは、この中の１つ、例えば「健康管理システム」４０２をカーソル移動によって選択する。

【００４５】なお、暗号化中継サービス自体も図４の選択画面４０１で選択する。図４においては、既に暗号化中継サービスが選択され、次に健康管理システムを選択した状態を示している。

【００４６】次に、認証プログラム２０４は、ユーザ名称とパスワードを入力する画面を表示する（ステップ３０２）。この入力画面５０１には、図５に示すように、ユーザ名称５０２とパスワード５０３の入力エリアが表示される。ユーザは、これらの入力エリアにユーザ名称５０２とパスワード５０３を入力する。

【００４７】次に、認証プログラム２０４は、ユーザから入力されたユーザ名称５０２とパスワード５０３を取り込む（ステップ３０３）。この後、認証サービスプログラム２０２に接続し（ステップ３０４）、取り込んだユーザ名称５０２とパスワード５０３のペアと、認証後に起動するクライアントプログラム（健康管理システム）２０３が中継サービスプログラム２０１に接続する時のＴＣＰ／ＩＰポートを認証サービスプログラム２０２に送信する（ステップ３０５）。

【００４８】次に、認証サービスプログラム２０２から認証の結果を受信する（ステップ３０６）。そして、受信した結果をチェックし（ステップ３０７）、「ＮＧ」であれば、ステップ３０３から繰り返す。「ＯＫ」であれば、クライアントプログラム（健康管理システム）２０３を起動し（ステップ３０８）し、終了する。

【００４９】図６は、認証サービスプログラム２０２の動作を示すフローチャートである。

【００５０】まず、認証サービスプログラム２０２は、クライアントコンピュータ２のユーザＤＢ２０７内に設けられ、ユーザ名称とパスワードのペアを格納しているファイルを開き、その内容をメモリ中に読み込む（ステップ６０１）。

【００５１】次に、ＴＣＰ／ＩＰポートの「３００１番」と「３００２番」を用意し、認証プログラム２０４または中継サービスプログラム２０１からの接続を待つ（ステップ６０２）。

【００５２】次に、接続元が認証プログラム２０４か、中継サービスプログラム２０１かをチェックする（ステップ６０３）。接続元が認証プログラム２０４であった場合、ユーザが入力した「ユーザ名称」５０２と「パスワード」５０３、クライアントプログラム（健康管理システム）２０３が使用する中継サービスプログラム２０１のＴＣＰ／ＩＰポート番号を受信する（ステップ６０４）。

【００５３】その後、受信したユーザ名称５０２とパスワード５０３とが、ユーザＤＢ２０７のファイルから読み込んだユーザ名称とパスワードの群の中にあるかどうかをチェックする（ステップ６０５）。もし、群の中になかった場合は、認証プログラム２０４に「ＮＧ」を送信し（ステップ６０６）、ステップ６０２からの処理を繰り返す。

【００５４】もし、群の中にあった場合は、乱数を使用し、今回の接続に対する固有の暗号鍵を生成し、中継サービスプログラム２０１のポート番号とともにメモリ中に保持しておき、認証プログラム２０４に「ＯＫ」を送信し（ステップ６０７）、ステップ６０２からの処理を繰り返す。

【００５５】接続元が中継サービスプログラム２０１であった場合は、まず、中継サービスプログラム２０１から中継サービス２０１が使用しているポート番号と中継の開始か終了かを示すフラグを受信する（ステップ６０８）。

【００５６】中継開始の場合は、保持していた中継サービスプログラム２０１のポート番号と暗号鍵のペアを調べ、対応する暗号鍵を中継サービスプログラム２０１に送信する（ステップ６０９，６１０）。中継終了の場合は、中継サービスプログラム２０１のポート番号に対応する暗号鍵をメモリ中から破棄し（ステップ６１１）、ステップ６０２からの処理を繰り返す。

【００５７】図７は、クライアントコンピュータ２上で稼動する中継サービスプログラム２０１の動作を示すフローチャートである。

【００５８】クライアントコンピュータ２上で稼動する中継サービスプログラム２０１は、複数の中継用のＴＣＰ／ＩＰポートを用意し、クライアントプログラム（健康管理システム）２０３からの接続を待つ（ステップ７０１）。

【００５９】クライアントプログラム（健康管理システム）２０３から接続されると、認証サービスプログラム２０２に接続し、ポート番号と中継開始のフラグを認証サービスプログラム２０２に送信する（ステップ７０２）。

【００６０】次に、認証サービスプログラム２０２から暗号鍵を受信する（ステップ７０３）。

【００６１】次に、サーバコンピュータ１上の中継サービスプログラム２０５と接続し、中継サービス固有の鍵で認証サービスプログラム２０２から受信した暗号鍵を暗号化して送信する（ステップ７０４）。

【００６２】次に、クライアントプログラム（健康管理システム）２０３またはサーバコンピュータ１上の中継サービスプログラム２０５からデータが送信されてくるのを待つ（ステップ７０５）。

【００６３】クライアントプログラム（健康管理システム）２０３からデータを受信した場合は、その受信したデータが「送信終了」のデータであるかどうかをチェックする（ステップ７０６）。

【００６４】「送信終了」であれば、再度、認証サービスプログラム２０２に接続して中継用のポート番号と中継終了用のフラグを送信した後、クライアントプログラム（健康管理システム）２０３とサーバコンピュータ１上の中継サービスプログラム２０５との接続を切断し（ステップ７０７）、ステップ７０１からの処理を繰り返す。

【００６５】受信データが通常のデータであれば、そのデータを暗号鍵で暗号化し、サーバコンピュータ１の中継サービスプログラム２０５に送信し（ステップ７０８）、ステップ７０５からの処理を繰り返す。

【００６６】サーバコンピュータ１上で稼動する中継サービスプログラム２０５からデータを受信した場合は、そのデータを暗号鍵で復号し、クライアントプログラム（健康管理システム）２０３に送信し（ステップ７０９）、ステップ７０５からの処理を繰り返す。

【００６７】図８は、サーバコンピュータ１上で稼動する中継サービスプログラム２０５の動作を示すフローチャートである。

【００６８】サーバコンピュータ１上で稼動する中継サービスプログラム２０５は、複数の中継用のＴＣＰ／ＩＰポートを用意し、クライアントコンピュータ２上で稼動する中継サービスプログラム２０１からの接続を待つ（ステップ８０１）。

【００６９】クライアントコンピュータ２で稼動する中継サービスプログラム２０１から接続されると、まず、暗号鍵を受信し、その暗号鍵を中継サービス固有の鍵で復号してメモリ中に保持しておく（ステップ８０２）。

【００７０】次に、サーバプログラム２０６と接続し（ステップ８０３）、サーバプログラム２０６またはクライアントコンピュータ１上の中継サービスプログラム２０１からデータが送信されてくるのを待つ（ステップ８０４）。

【００７１】クライアントコンピュータ２上で稼動する中継サービスプログラム２０１からデータを受信した場合は、その受信したデータが「通信終了」のデータかど

うかをチェックする（ステップ８０５）。「通信終了」のデータであれば、サーバプログラム２０６とクライアントコンピュータ２上の中継サービスプログラム２０１との接続を切断し（ステップ８０６）、ステップ８７０１からの処理を繰り返す。

【００７２】受信したデータが通常のデータであれば、そのデータをステップ８０２で入手した暗号鍵で復号し、サーバプログラム２０６に送信し（ステップ８０７）、ステップ８０４からの処理を繰り返す。

【００７３】サーバプログラム２０６からデータを受信した場合は、そのデータをステップ８０２で入手した暗号鍵で暗号化し、クライアントコンピュータ１上で稼動する中継サービスプログラム２０１に送信し（ステップ７０８）、ステップ８０４からの処理を繰り返す。

【００７４】このように、本実施形態によれば、サーバコンピュータ１およびクライアントコンピュータ２に中継サービスプログラム２０１，２０２を組み込み、この中継サービスプログラム２０１，２０２によって両コンピュータ間のデータを暗号化して通信するようにしているため、ネットワークがバス形式であっても、既設のクライアントプログラム２０３やオペレーティングシステムに全く変更を加えることなく、ネットワーク３を経由したデータのセキュリティを確保することができる。

【００７５】また、中継サービスプログラム２０１，２０２は、起動プログラムによって稼働状態と非稼働状態に任意に切替えることができるため、非稼働状態にしておくことにより、暗号化しないデータを送受信することもできる。

【００７６】さらに、中継サービスプログラム２０１，２０２は、フロッピイディスクやＣＤ－ＲＯＭ等の記録媒体に記録されてユーザに提供されるため、ユーザは所有するコンピュータ内にハードウェア空間が残っていなくても、中継サービスプログラム２０１，２０２をメモリ内に組み込むのみの操作で、既設のアプリケーションプログラムやオペレーティングシステムを全く変更することなく、暗号化したデータを送受信することが可能になる。

【００７７】さらに、本実施形態では、認証サービスプログラム２０２を設け、クライアントコンピュータ２を使用するユーザの認証を個人単位で行い、かつ個人単位の暗号鍵を生成し、その個人単位の暗号鍵によってデータを暗号化して送信しているため、クライアントコンピュータ２を使用する複数のユーザ間でもデータのセキュリティを確保することができる。

【００７８】なお、図１においては、サーバコンピュータ１とクライアントコンピュータ２との間でのデータ通信について説明したが、本発明はこれに限定されるものではなく、図９に示すように、ネットワーク３に接続された複数のパーソナルコンピュータ（ＰＣ）９１，９２、携帯型の情報家電（情報端末）９３，９４、ワークステーション９５の中に組み込んで使用することができる。

【００７９】また、認証サービスプログラム２０２は、必要に応じて付加するようにしてもよい。

【００８０】さらに、クライアントコンピュータ２とサーバコンピュータ１間の通信は必ず中継サービスプログラム２０１，２０５を経由するため、各コンピュータ間で通信されるデータに関してログをとるようにしてもよい。

【００８１】また、個人単位の暗号鍵で暗号化する際の暗号アルゴリズムを、健康管理システム、社員検索システムなどのクライアントプログラム別に異ならせる、あるいはユーザ別に異ならせ、高度のセキュリティを必要とするもの程、復号が困難になるようにしてもよい。

【００８２】

【発明の効果】以上説明したように本発明によれば、データを通信するコンピュータ内に中継サービスプログラムを組み込み、この中継サービスプログラムによって他のコンピュータとの間で送受信するデータを暗号化するようにしているため、ネットワークがバス形式であっても、既設のアプリケーションプログラムやオペレーティングシステムに全く変更を加えることなく、ネットワークを経由したデータのセキュリティを確保することができる。

【００８３】また、中継サービスプログラムは、起動プログラムによって稼働状態と非稼働状態に任意に切替えることができるため、非稼働状態にしておくことにより、暗号化しないデータを送受信することもできる。

【００８４】さらに、中継サービスプログラムは、フロッピイディスクやＣＤ－ＲＯＭ等の記録媒体に記録されてユーザに提供されるため、ユーザは所有するコンピュータ内にハードウェア空間が残っていなくても、中継サービスプログラムをメモリ内に組み込むのみの操作で、既設のアプリケーションプログラムやオペレーティングシステムを全く変更することなく、暗号化したデータを送受信することが可能になる。

【００８５】さらに、認証サービスプログラムを組み込み、ユーザの認証を個人単位で行い、かつ個人単位の暗号鍵を生成し、その個人単位の暗号鍵によってデータを暗号化して送信するように構成した場合には、同じコンピュータを使用する複数のユーザ間でもデータのセキュリティを確保することができる。

【図面の簡単な説明】

【図１】本発明を適用した暗号化データ通信システムの実施形態を示すシステム構成図である。

【図２】図１の実施形態における中継サービスプログラムを利用した通信時のデータの流れを示す図である。

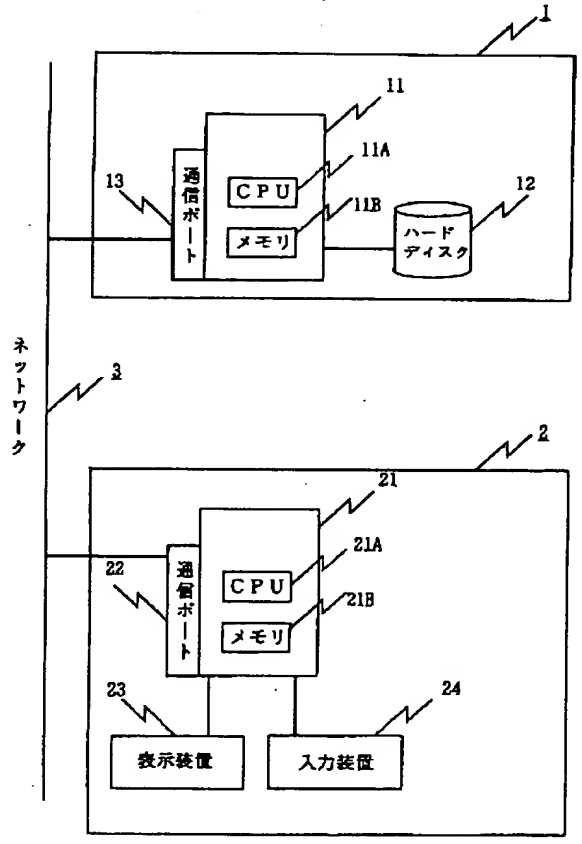
【図３】クライアントコンピュータに組み込まれた認証プログラムの処理手順を示すフローチャートである。

【図４】認証プログラムが表示するシステム選択画面の

例を示す説明図である。
【図５】認証プログラムが表示するユーザ名称等の入力画面の例を示す説明図である。
【図６】クライアントコンピュータに組み込まれた認証サービスプログラムの処理手順を示すフローチャートである。
【図７】クライアントコンピュータ上で稼動する中継サービスプログラムの処理手順を示すフローチャートである。
【図８】サーバコンピュータ上で稼動する中継サービスプログラムの処理手順を示すフローチャートである。
【図９】本発明の適用するコンピュータの他の例を示すネットワーク構成図である。
【符号の説明】
１…サーバコンピュータ、１１…端末装置、１１Ａ…ＣＰＵ、１１Ｂ…メモリ、１２…ハードディスク、１３…通信ポート、２…クライアントコンピュータ、２１…端末装置、２１Ａ…ＣＰＵ、２１Ｂ…メモリ、２２…ハードディスク、２３…通信ポート、２４…表示装置、２５…入力装置、３…ネットワーク。

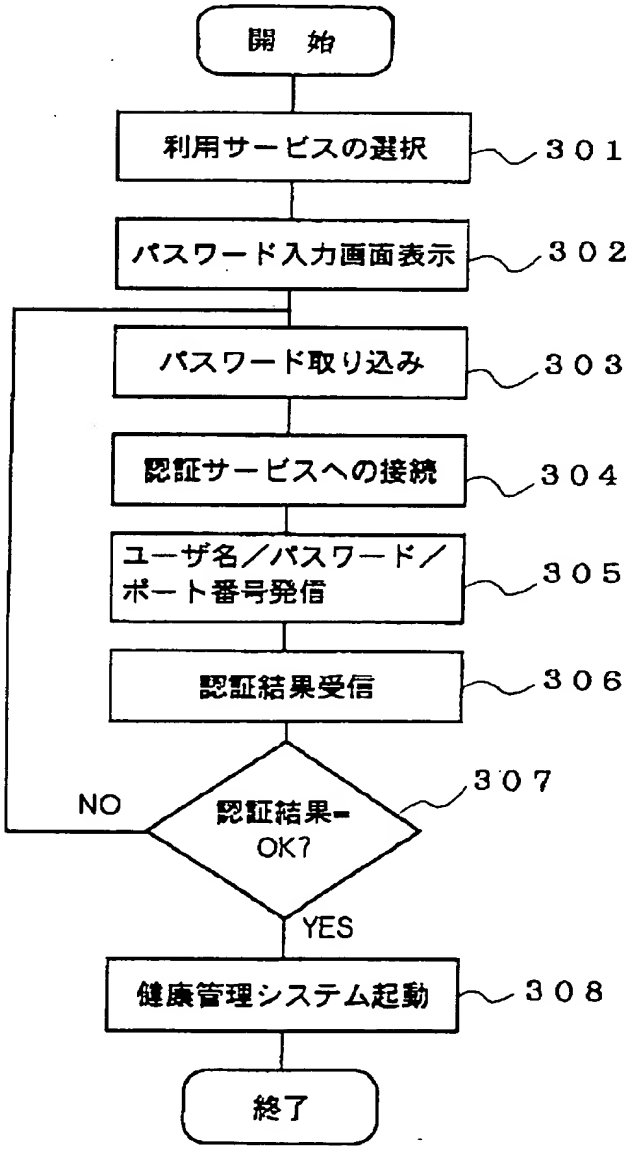
【図１】

図１



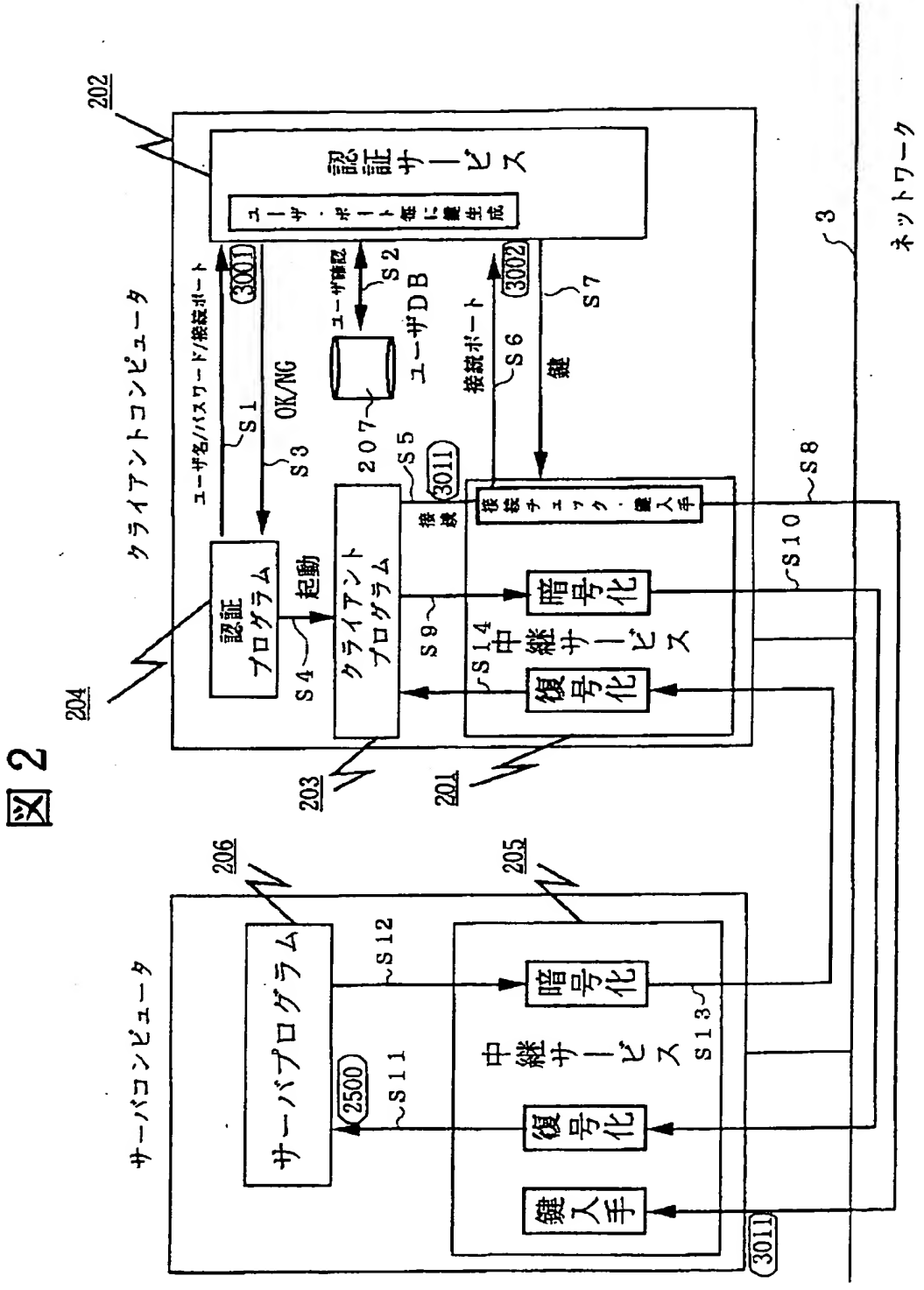
【図３】

図３



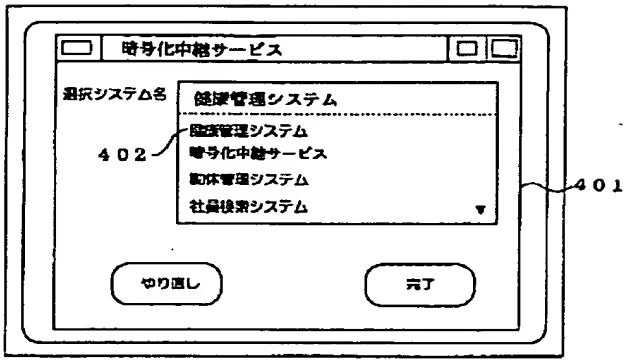
【図２】

図２


202
認証サービス
ユーザ・ポートに鍵生成
クライアントコンピュータ
ユーザ名/パスワード/接続ポート
3001
S1
OK/NG
S3
ユーザ確認
S2
ユーザDB
207
S5
3011
接続
接続ポート
S6
3002
鍵
S7
3
ネットワーク
S8
接続チェック・鍵入手
認証プログラム
起動
S4
クライアントプログラム
S9
暗号化
S14
中継サービス
復号化
S10
204
203
201
206
205
サーバコンピュータ
サーバプログラム
S12
暗号化
中継サービス
S13
2500
S11
復号化
鍵入手
3011

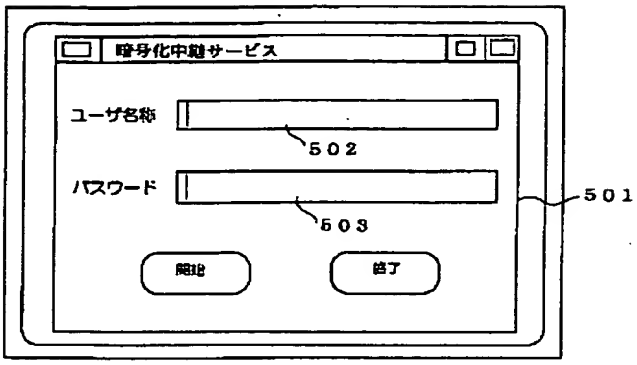
【図４】

図４



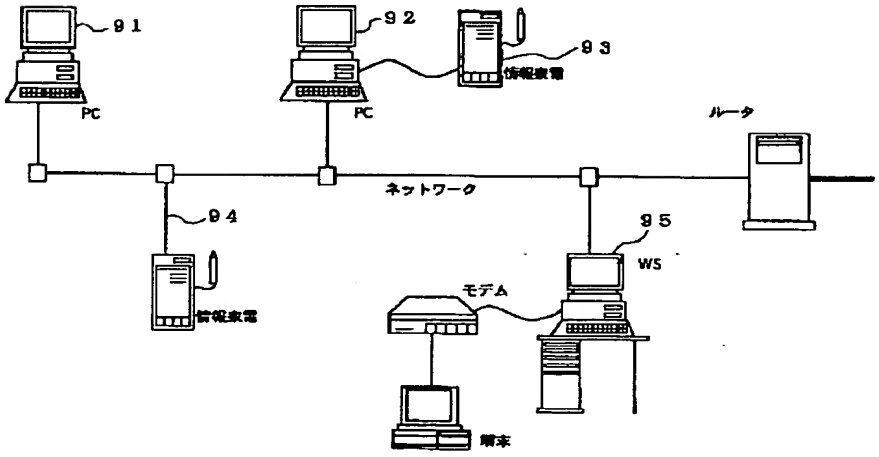
【図５】

図５



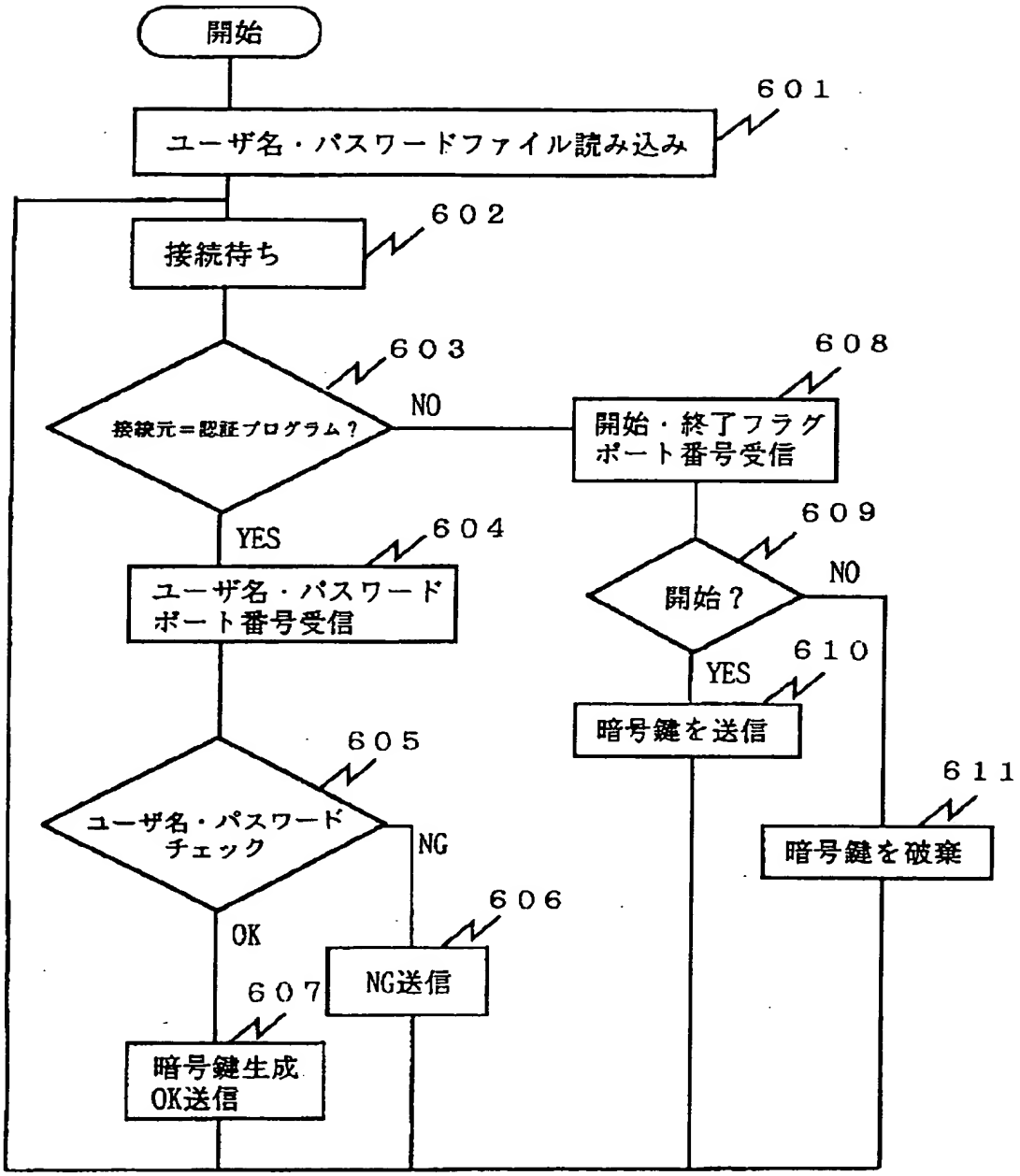
【図９】

図９



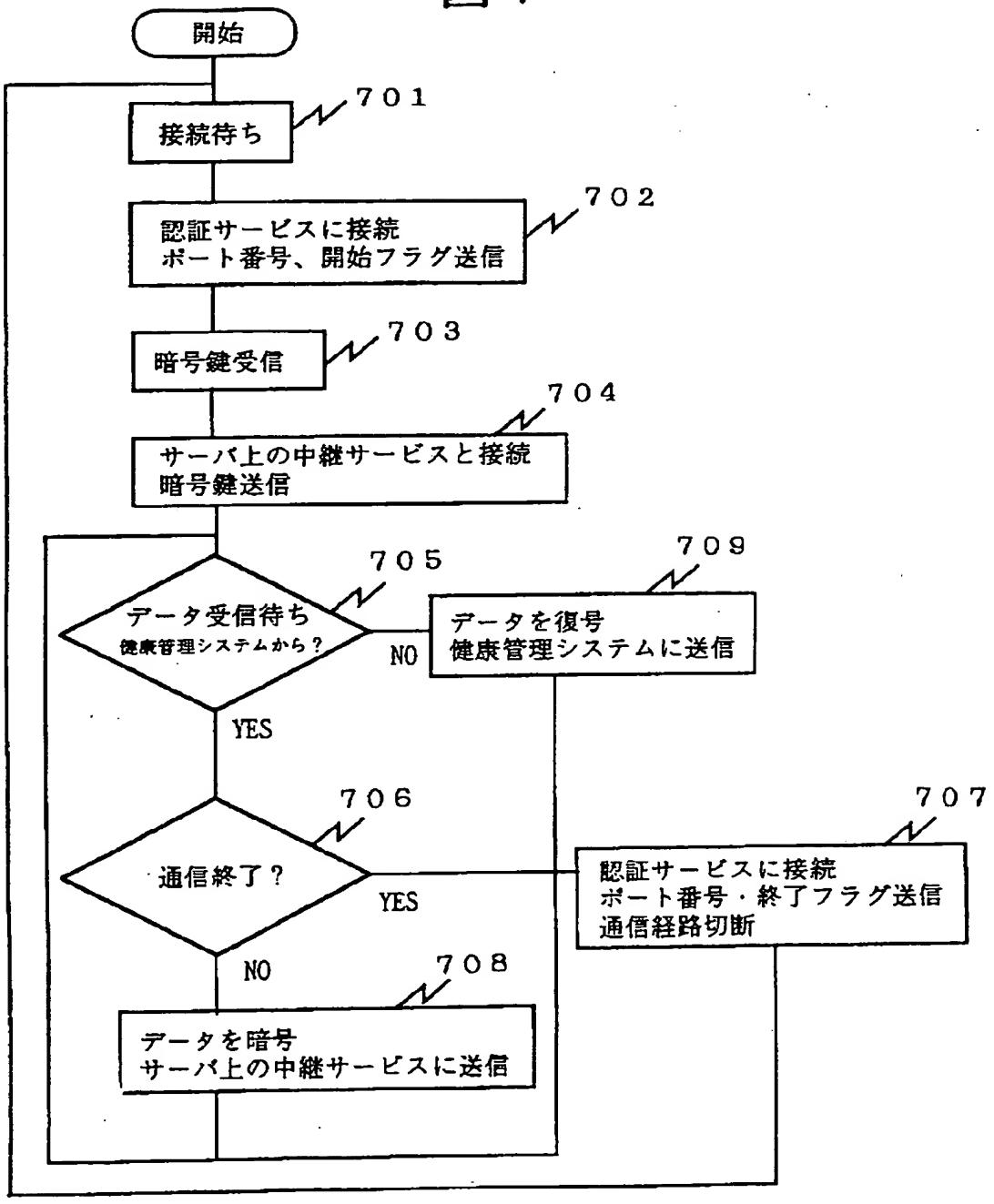
【図６】

図６


開始
601
ユーザ名・パスワードファイル読み込み
602
接続待ち
603
接続元＝認証プログラム？
NO
608
開始・終了フラグ
ポート番号受信
YES
604
ユーザ名・パスワード
ポート番号受信
609
開始？
NO
YES
610
暗号鍵を送信
605
ユーザ名・パスワード
チェック
NG
611
暗号鍵を破棄
606
OK
NG送信
607
暗号鍵生成
OK送信

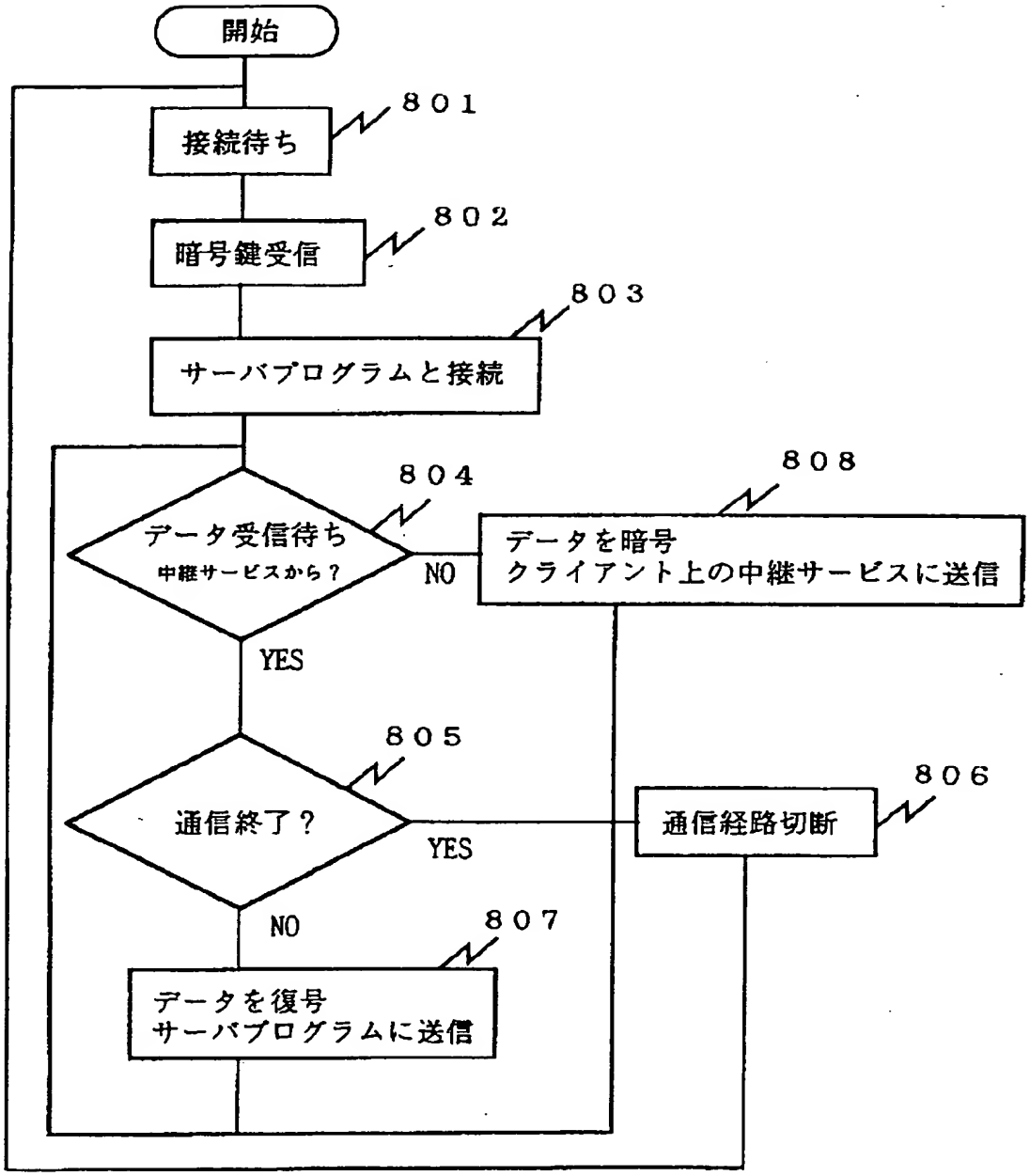
【図7】

図7


開始
701
接続待ち
702
認証サービスに接続
ポート番号、開始フラグ送信
703
暗号鍵受信
704
サーバ上の中継サービスと接続
暗号鍵送信
705
データ受信待ち
健康管理システムから？
NO
709
データを復号
健康管理システムに送信
YES
706
通信終了？
YES
707
認証サービスに接続
ポート番号・終了フラグ送信
通信経路切断
NO
708
データを暗号
サーバ上の中継サービスに送信

【図８】

図８


開始
801
接続待ち
802
暗号鍵受信
803
サーバプログラムと接続
804
データ受信待ち
中継サービスから？
NO
808
データを暗号
クライアント上の中継サービスに送信
YES
805
通信終了？
YES
806
通信経路切断
NO
807
データを復号
サーバプログラムに送信